

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with three target accounts that
are stored at premises controlled by Microsoft Corp,
as more fully described in Attachment A-3

Case No. MJ23-411

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Information associated with three target accounts that are stored at premises controlled by Microsoft Corp, as more fully described in Attachment A-3, incorporated herein by reference

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B-3, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1343	Wire Fraud

The application is based on these facts:

- ☒ See Affidavit of FBI Special Agent Kathleen Moran, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

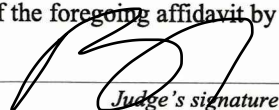
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.


Applicant's signature

Kathleen Moran, FBI Special Agent
Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 08/18/2023


Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida U.S. Magistrate Judge
Printed name and title

[illegible]

I, Kathleen Moran, a Special Agent of the Federal Bureau of Investigation, being first duly sworn, depose and state as follows:

1. This affidavit is submitted in support of an application for search warrants for retained communications and other records of the following 31 email accounts used to fraudulently obtain or attempt to obtain rental assistance funds from a federally funded COVID-19 pandemic relief program:

1. David.martinez.ceo@outlook.com (Account 1)
2. Shirleywilliamhomes@outlook.com (Account 2)
3. raypeterson206@outlook.com (Account 3)
4. malikahproperties@gmail.com (Account 4)
5. mauricehunterhomes@gmail.com (Account 5)
6. cartellale@gmail.com (Account 6)
7. AnisaHaji904@gmail.com (Account 7)
8. Ashleymarie081590@gmail.com (Account 8)
9. bodiedexperience@gmail.com (Account 9)
10. akimjackson3@gmail.com (Account 10)
11. shirleyme63@gmail.com (Account 11)
12. minahcunning@gmail.com (Account 12)
13. Sequoyahillsestate.homes@gmail.com (Account 13)
14. akialwatson@gmail.com (Account 14)
15. huntersandra027@gmail.com (Account 15)
16. amyadon2000@gmail.com (Account 16)
17. islynnkj@gmail.com (Account 17)
18. kowserkassa30@gmail.com (Account 18)
19. abdihomesguy@gmail.com (Account 19)
20. samiaabdulwahab@gmail.com (Account 20)
21. mohhsemhar916@gmail.com (Account 21)
22. ishakayla.homes12@gmail.com (Account 22)
23. mtajaraye@gmail.com (Account 23)
24. hibbitalvina@gmail.com (Account 24)
25. wawoman445@gmail.com (Account 25)

26. shemshiameriam@yahoo.com (Account 26)
27. shawpropertymg@yahoo.com (Account 27)
28. tiarobinson437@yahoo.com (Account 28)
29. terrellhouston123@yahoo.com (Account 29)
30. jacksonrodney206@yahoo.com (Account 30)
31. qubahawkins1991@icloud.com (Account 31)

(collectively, the “Subject Email Accounts”).

2. Defendants Paradise Williams, D’arius Jackson, Jahri Cunningham, Tia Robinson, Rayvon Peterson, and David Martinez were indicted on May 31, 2023 on wire fraud and money laundering charges. From about June 2020 until February 2022, the defendants, and others, fraudulently sought more than \$6.8 million, and obtained more than \$3.3 million, from various federally funded COVID-19 pandemic relief programs, to include the U.S. Department of Treasury’s Emergency Rental Assistance program administered through Washington State grant programs and King County Eviction Prevention and Rental Assistance Program (EPRAP).

3. The Subject Email Accounts are email accounts that were used by the defendants and others to access or attempt to access the EPRAP program as fictitious landlords, and to receive communications from the EPRAP program, including the agreement the landlords needed to sign before receiving funds. The email accounts may also contain communications between the defendants and others regarding the fake documents and information they submitted or planned to submit to King County. Because the Subject Email Accounts were used to obtain or attempt to obtain ERPAP funds, the accounts may contain communications related to the use of those funds, and whether any funds were given to Paradise Williams in exchange for orchestrating the scheme.

4. The facts set forth in this Affidavit are based on information obtained by me and others during this investigation from a variety of sources, including, but not limited to: (a) information provided to me by King County; (b) business records and other documents obtained from various entities; and (c) publicly available documents.

1 5. Because this Affidavit is submitted for the limited purpose of establishing
2 probable cause in support of the application for a search warrant, it does not set forth
3 each and every fact that I or others have learned during the course of this investigation. I
4 have set forth only the facts that I believe are necessary to establish probable cause to
5 believe that evidence, fruits and instrumentalities of violations of Title 18, United States
6 Code, Section 1343 (Wire Fraud) will be found within the Subject Email Accounts.

7 **II. EXPERIENCE OF AGENT**

8 6. I am a Special Agent of the Federal Bureau of Investigation ("FBI")
9 currently assigned to the white-collar crime squad in the Seattle Field Division. I have
10 been employed as a Special Agent of the FBI since May 2005. I have received basic
11 federal law enforcement training, including the training at the FBI Academy, as well as
12 other specialized federal law enforcement training. I have investigated violations of
13 federal statutes governing various types of white-collar crime, including wire fraud, mail
14 fraud, bank fraud, securities fraud, money laundering, and theft of government and public
15 money.

16 **III. LOCATION TO BE SEARCHED**

17 7. I make this affidavit in support of an application for search warrants,
18 pursuant to Federal Rule of Criminal Procedure 41, and Title 18, United States Code,
19 Section 2703, to search the electronic communications contained in, as well as all
20 subscriber and log records associated with, the Subject Email Accounts.

21 8. The Gmail accounts are located on the premises owned, maintained,
22 controlled, or operated by Google LLC ("Google"), an electronic communications service
23 and/or remote computing service provider located at 1600 Amphitheatre Parkway,
24 Mountain View, California, 94043, as further described in Attachment A-1, attached
25 hereto and incorporated herein.

26 9. The Yahoo accounts are located on the premises owned, maintained,
27 controlled, or operated by Yahoo Inc. ("Yahoo"), an electronic communications service
28 and/or remote computing service provider headquartered at 70 Broadway, 9th Floor, New

1 York, New York 10003, with its custodian of records located at 391 San Antonio Road,
2 5th Floor, Mountain View, California 94040, as further described in Attachment A-2,
3 attached hereto and incorporated herein.

4 10. The Outlook accounts are located on the premises owned, maintained,
5 controlled, or operated by Microsoft Corporation ("Microsoft"), an electronic
6 communications service and/or remote computing service provider located at One
7 Microsoft Way, Redmond, Washington, 98052, as further described in Attachment A-3,
8 attached hereto and incorporated herein.

9 11. The iCloud account is located on the premises owned, maintained,
10 controlled, or operated by Apple Inc. ("Apple"), an electronic communications service
11 and/or remote computing service provider headquartered at One Apple Park Way,
12 Cupertino, California, as further described in Attachment A-4, attached hereto and
13 incorporated herein.

14 12. Through their email services, "gmail.com," "yahoo.com," and
15 "outlook.com," "icloud.com", Google, Yahoo, Microsoft, and Apple provide free email
16 addresses and online email storage to its subscribers. In my training and experience, I
17 have learned that Google, Yahoo, Microsoft, and Apple provide a variety of on-line
18 services, including electronic mail ("email") access, to the public. Google, Yahoo,
19 Microsoft, and Apple allow subscribers to obtain email accounts at the domain name
20 (e.g., gmail.com, yahoo.com, outlook.com, icloud.com), like the Subject Email Accounts
21 listed in Attachment A-1 through A-4. Subscribers obtain an account by registering with
22 Google, Yahoo, Microsoft, and Apple. During the registration process, Google, Yahoo,
23 Microsoft, and Apple ask subscribers to provide basic personal information. Therefore,
24 the computers of Google, Yahoo, Microsoft, and Apple are likely to contain stored
25 electronic communications (including retrieved and unretrieved email for Google, Yahoo,
26 Microsoft, and Apple subscribers and information concerning subscribers and their use of
27 Google, Yahoo, Microsoft, and Apple services, such as account access information, email
28 transaction information, and account application information. In my training and

1 experience, such information may constitute evidence of the crimes under investigation
2 because the information can be used to identify the account's user or users.

3 13. A Google, Yahoo, Microsoft and Apple subscriber can also store with the
4 provider files in addition to emails, such as address books, contact or buddy lists,
5 calendar data, pictures (other than ones attached to emails), and other files, on servers
6 maintained and/or owned by Google, Yahoo, Microsoft, and Apple. In my training and
7 experience, evidence of who was using an email account may be found in address books,
8 contact or buddy lists, email in the account, and attachments to emails, including pictures
9 and files.

10 14. In my training and experience, email providers generally ask their
11 subscribers to provide certain personal identifying information when registering for an
12 email account. Such information can include the subscriber's full name, physical address,
13 telephone numbers and other identifiers, alternative email addresses, and, for paying
14 subscribers, means and source of payment (including any credit or bank account number).
15 In my training and experience, such information may constitute evidence of the crimes
16 under investigation because the information can be used to identify the account's user or
17 users. Based on my training and my experience, I know that, even if subscribers insert
18 false information to conceal their identity, this information often provides clues to their
19 identity, location, or illicit activities.

20 15. In my training and experience, email providers typically retain certain
21 transactional information about the creation and use of each account on their systems.
22 This information can include the date on which the account was created, the length of
23 service, records of log-in (*i.e.*, session) times and durations, the types of service utilized,
24 the status of the account (including whether the account is inactive or closed), the
25 methods used to connect to the account (such as logging into the account via the
26 provider's website), and other log files that reflect usage of the account. In addition,
27 email providers often have records of the Internet Protocol address ("IP address") used to
28 register the account and the IP addresses associated with particular logins to the account.

1 Because every device that connects to the Internet must use an IP address, IP address
2 information can help to identify which computers or other devices were used to access
3 the email account.

4 16. In my training and experience, in some cases, email account users will
5 communicate directly with an email service provider about issues relating to the account,
6 such as technical problems, billing inquiries, or complaints from other users. Email
7 providers typically retain records about such communications, including records of
8 contacts between the user and the provider's support services, as well as records of any
9 actions taken by the provider or user as a result of the communications. In my training
10 and experience, such information may constitute evidence of the crimes under
11 investigation because the information can be used to identify the account's user or users.

12 17. As explained herein, information stored in connection with an email account
13 may provide crucial evidence of the "who, what, why, when, where, and how" of the
14 criminal conduct under investigation, thus enabling the United States to establish and
15 prove each element or alternatively, to exclude the innocent from further suspicion. In my
16 training and experience, the information stored in connection with an email account can
17 indicate who has used or controlled the account. This "user attribution" evidence is
18 analogous to the search for "indicia of occupancy" while executing a search warrant at a
19 residence. For example, email communications, contacts lists, and images sent (and the
20 data associated with the foregoing, such as date and time) may indicate who used or
21 controlled the account at a relevant time. Further, information maintained by the email
22 provider can show how and when the account was accessed or used. For example, as
23 described below, email providers typically log the Internet Protocol (IP) addresses from
24 which users access the email account, along with the time and date of that access. By
25 determining the physical location associated with the logged IP addresses, investigators
26 can understand the chronological and geographic context of the email account access and
27 use relating to the crime under investigation. This geographic and timeline information
28 may tend to either inculcate or exculpate the account owner. Additionally, information

1 stored at the user's account may further indicate the geographic location of the account
2 user at a particular time (*e.g.*, location information integrated into an image or video sent
3 via email). Last, stored electronic data may provide relevant insight into the email
4 account owner's state of mind as it relates to the offense under investigation. For
5 example, information in the email account may indicate the owner's motive and intent to
6 commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt
7 (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

8 18. This application seeks warrants to search the Subject Email Accounts, as
9 described in Attachments A-1 through A-4, and seize the items listed in Attachments B-1
10 through B-4, which are attached to this affidavit and incorporated herein by reference for
11 evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1343 (Wire
12 Fraud).

13 IV. BACKGROUND

14 A. Emergency Rental Assistance

15 19. In response to millions of Americans facing deep rental debt, fear of
16 evictions, and the loss of basic housing security as a result of the COVID-19 pandemic,
17 the U.S. Department of Treasury's Emergency Rental Assistance program provided
18 funding directly to state and local governments to assist households that were unable to
19 pay rent or utilities. From March 2021 through 2022, Treasury's Emergency Rental
20 Assistance program allocated over \$900 million to Washington State and local
21 governments, including King County. The Washington Department of Commerce
22 received and administered the state's federal funds by providing grants to county
23 governments and non-profit organizations to support the homeless crisis response
24 systems in the state. In King County, the Department of Community and Human
25 Services distributed over \$300 million in direct federal funds and state grants to
26 approximately 30,000 King County households through EPRAP.

27 20. To qualify for rental assistance, the household must have been low-income,
28 experiencing financial hardship due to the COVID-19 pandemic, and been at risk of

1 experiencing homelessness or currently experiencing housing instability. Tenants and
2 landlords could receive up to 12 months of rental assistance (nine months back or current
3 rent and three months advance). The administering agencies acknowledged that there
4 was insufficient funding to help every household who qualified, thus, the screening
5 criteria was intended to target those most likely to become homeless but for the
6 assistance.

7 21. In King County, a landlord could initiate an application for EPRAP
8 assistance by submitting a delinquent tenant's information, and the tenant and landlord
9 could submit self-attestation forms to document eligibility. Landlords were also required
10 to submit W-9 forms and, upon request, evidence of a lease or ledger. After EPRAP
11 calculated the final assistance amount, landlords received an EPRAP agreement by email
12 that they were required to sign and return via DocuSign using interstate wire
13 transmissions. The agreement certified that the signee was authorized to accept the
14 emergency rental assistance payment in satisfaction of rent owed by a tenant.

15 22. King County initiated payment of the EPRAP funds by using an interstate
16 wire to upload payment information to a bank server located outside Washington State.
17 EPRAP funds were disbursed to landlords via checks or ACH payments using interstate
18 wire transmissions.

19 23. Paradise Williams orchestrated the scheme to defraud the EPRAP program,
20 and she directed D'arius Jackson, Jahri Cunningham, Tia Robinson, Rayvon Peterson,
21 David Martinez, and others to use their true identities and aliases, to pose fraudulently as
22 landlords for property located within King County, and to obtain rental assistance for
23 non-existent tenants. Williams, Jackson, Cunningham, Robinson, Peterson, Martinez,
24 and others created and used multiple email accounts and Voice over Internet Protocol
25 (VoIP) phone numbers in furtherance of the scheme. They created and used fake rental
26 agreements, ledgers, and other documents to support the fraudulent applications.
27 Williams, Jackson, Cunningham, Robinson, Peterson, and Martinez impersonated and
28 directed others to impersonate fictitious tenants and landlords when EPRAP staff

1 contacted them by phone, text, or email. Williams, Robinson, and Peterson received
2 kickback payments for applications they submitted on behalf of other fictitious landlords.
3 Martinez, and others, paid Williams kickbacks for the applications she submitted using
4 their identities.

5 24. In total, between approximately August 27, 2021 and February 11, 2022,
6 Williams, Jackson, Cunningham, Robinson, Peterson, Martinez and others submitted over
7 78 EPRAP applications, seeking over \$2.8 million and obtaining over \$2.7 million in
8 federal Emergency Rental Assistance funds.

9 **B. Indictment**

10 25. On May 31, 2023, in a 26-count Indictment, the Grand Jury charged Paradise
11 Williams, D'arius Jackson, Jahri Cunningham, Tia Robinson, Rayvon Peterson, and
12 David Martinez with wire fraud for fraudulently obtaining more than \$3.3 million from
13 federally funded COVID-19 pandemic relief programs: EPRAP, the Paycheck Protection
14 Program (PPP) administered by the U.S. Small Business Administration (SBA), and the
15 Economic Injury Disaster Loan (EIDL) Program administered by the SBA. The
16 defendants were also charged with money laundering. On June 5, 2023, the defendants
17 were arrested by the FBI in various jurisdictions, and the last defendant was arraigned on
18 July 20, 2023.

19 **V. RELEVANCE OF SUBJECT EMAIL ADDRESSES**

20 26. According to information provided by King County, the EPRAP process was
21 typically initiated by a tenant accessing King County's on-line portal and answering some
22 preliminary questions, such as name, address, household size, and income. The
23 information was routed to a data system, which started the application. The tenant then
24 provided their landlord's information, including the landlord's phone number, contact
25 information, and email. An email message was automatically sent by King County to the
26 landlord to notify the landlord of the tenant's interest and to direct the landlord to the
27 portal, where the landlord submitted the required information.
28

27. In addition to receiving the initial notification by email, after EPRAP calculated the final assistance amount, landlords received an EPRAP agreement by email that they were required to sign and return via DocuSign. The agreement certified that the signee was authorized to accept the emergency rental assistance payment in satisfaction of rent owed by a tenant.

28. As detailed in the attached Exhibit 1, the Subject Email Addresses were submitted to King County's database for the fictitious landlords portrayed by Paradise Williams, D'arius Jackson, Jahri Cunningham, Tia Robinson, Rayvon Peterson, David Martinez, and others associated with them. With the exception of A.P. and R.J., in every instance, the fictitious landlord did not own the property address submitted on the EPRAP application for the fake tenant.

29. A.P. is Rayvon Peterson's sister. While A.P. owns the property address submitted on the EPRAP application, she did not have Tenant 34, as represented to King County. Instead, Rayvon Peterson impersonated Tenant 34, at the direction of Paradise Williams, as described in text messages obtained through a search of Paradise Williams's phone, seized pursuant to a search warrant:

WILLIAMS	I gave your number to this guy that helps with rental assistance i been emailing him his band is Andrew
WILLIAMS	I did the app under the [Tenant 34] guy name
R. PETERSON	Waiting for this move, it has to go thru 🍷 my car note gonna be pullin from my acct at midnight 😬
WILLIAMS	[redacted address] Kent WA 98032
R. PETERSON	What's the details
WILLIAMS	Your behind on rent you need help
WILLIAMS	Say you being like 5/6 months now
WILLIAMS	6/7
WILLIAMS	Tell him your daughter stays with your
WILLIAMS	You
R. PETERSON	[redacted]@yahoo.com

1	WILLIAMS	Yeah that's the email
2	R. PETERSON	What's [A.P.] email
3	R. PETERSON	They have her name and number
4	R. PETERSON	They might call after
5	WILLIAMS	Ashleymarie081586@gmail.com [Account 9]
6	WILLIAMS	How many months you say your behind
7	R. PETERSON	Haven't got that far
8	R. PETERSON	What's the monthly I?
9	WILLIAMS	2200
10	R. PETERSON	[Tenant 34's alleged daughter's name] January 20 2017
11	WILLIAMS	Huh
12	R. PETERSON	Daughter info lol
13	WILLIAMS	Lol
14	R. PETERSON	Proof of rental notice
15	R. PETERSON	Rent past due notice
16	WILLIAMS	Ok ledger?
17	R. PETERSON	You will see everything in the email
18		

30. On June 3, 2022, Magistrate Judge Mary Alice Theiler authorized the search of Williams' computers and devices. Documents found on Williams' computer further substantiated that A.P.'s EPRAP application was fraudulent. These documents included a rental ledger, affidavit of Covid-19 impacts, and EPRAP employer wage attestation, which were all completed for Tenant 34. Nearly identical documents for other fake tenants associated with Accounts 1, 2, 3, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 19, and 28 were found on Williams's computer.

31. R.J., the landlord associated with Account 30, shares the same last name as charged defendant D'arius Jackson, although it is unknown if he is a relative. While R.J. owns the property address submitted on the EPRAP application, there is probable cause

1 to believe the EPRAP application is fraudulent for several reasons. According to law
2 enforcement databases, the Social Security Number listed on the application for R.J. does
3 not exist. The bank account listed on the application, which received the EPRAP funds
4 intended for R.J., does not belong to R.J., but instead, belongs to the alleged tenant,
5 Tenant 76. I obtained these bank account statements, beginning in August 2021, and
6 Tenant 76's address on the statements is a Phoenix, Arizona address. According to law
7 enforcement databases, Tenant 76 moved to Arizona in June or July, 2021, several
8 months before Tenant 76's application for rental assistance was submitted in October
9 2021. The metadata on the lease agreement submitted to King County for Tenant 76 is
10 linked to a relative of Paradise Williams, Sk.H. Finally, Tenant 76 is an associate of
11 another fictitious landlord, B.L. (who is D'arius Jackson's current or former girlfriend),
12 and an associate of S.W., a friend of Paradise Williams.

13 32. In several instances, at least some of the Subject Email Accounts were used
14 to communicate directly with the employees who administered the EPRAP program. For
15 example, text messages from Paradise Williams's phone indicate that on October 5, 2021,
16 an employee requested that Paradise Williams, portraying a fictitious landlord named
17 Shaw Williams with an email address shawpropertymg@yahoo.com, send a copy of a
18 tenant's lease and ledger directly to the employee's email. Williams responded that same
19 day that she sent the email to the employee. Similarly, on February 8, 2022, Jahri
20 Cunningham texted Paradise Williams to "Email the stuff to the cartellalel@gmail.com
21 [Account 7] so we can email the lady the evictions notices and everything from the email
22 she already has on file we are done with the notices now." Cunningham, portraying a
23 fictitious landlord named Ale Cartel, used Account 7, cartellale@gmail.com (the typo in
24 the email address in his text was corrected in a follow-up text).

25 //

26 //

27 //

33. Text messages exchanged between Paradise Williams and Tia Robinson on October 29, 2021, discussed the creation of email addresses for other associates they recruited to portray fictitious landlords:

ROBINSON	[A.H.]
ROBINSON	[K.K.]
ROBINSON	[S.M.]
ROBINSON	Ima make an email in each one of their names
WILLIAMS	Ok they don't have to use their real names but okey don't matter lol

The email addresses using the names of A.H. (Account 8), K.K. (Account 19), and S.M. (Account 22), were submitted to King County for fictitious landlords.

34. A search of Paradise Williams's phone revealed further texts between Williams and other fictitious landlords similar to those above regarding the submission of fraudulent EPRAP applications. These text exchanges about the submission of fraudulent EPRAP applications occurred with individuals associated with or referencing Accounts 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22, 27, 28, and 31.

35. Additionally, Accounts 2, 4, 5, 13, 22, and 27 all have usernames that suggest the user is a landlord, property manager, or otherwise associated with real estate. However, none of the associated fictitious landlords for these accounts owned property in King County at the time of the EPRAP application submission associated with their emails. For example, Account 27 is "shawpropertymg@yahoo.com" and was used to submit applications associated with Williams as the landlord. However, Williams was neither a property manager nor owner. Likewise, the real identity of the fictitious landlord associated with Account 5—"mauricehunterhomes@gmail.com"—is also neither a property manager nor owner.

36. There is probable cause to believe these Subject Email Accounts may contain evidence relevant to the offense of wire fraud for a number of reasons. First,

1 because these email accounts were provided as contact email addresses to King County
2 for the fictitious landlords, the accounts are likely to contain communications between
3 King County and the fictitious landlords, including the email containing the EPRAP
4 agreement. Second, as revealed in the texts between Paradise Williams and Jahri
5 Cunningham, the Subject Email Accounts may contain communications between
6 Paradise Williams, D'arius Jackson, Jahri Cunningham, Tia Robinson, Rayvon Peterson,
7 David Martinez, and others regarding fake documents and information submitted to King
8 County. Finally, because the Subject Email Accounts were used to obtain EPRAP funds,
9 the accounts may contain communications related to the use of those funds, and whether
10 any funds were given to Paradise Williams in exchange for orchestrating the scheme.

11 **VI. PAST EFFORTS TO OBTAIN AND PRESERVE EVIDENCE.**

12 37. On June 30, 2021, United States Magistrate Judge Mary Alice Theiler
13 authorized a search warrant for email account David.martinez.ceo@outlook.com (one of
14 the Subject Email Accounts). The search warrant was based on EIDL and PPP fraud (the
15 EPRAP fraud was then unknown to investigators), and a search of the email account
16 indicated that Paradise Williams was the user of the account. Furthermore, the email
17 account David.martinez.ceo@outlook.com contained email communications from the
18 SBA regarding fraudulent EIDL and PPP applications submitted by Paradise Williams.
19 The fraudulent EPRAP applications were not initiated until August 2021 at the earliest,
20 thus, the June 30, 2021 search warrant of the David.martinez.ceo@outlook.com email
21 account did not cover the timeframe during which the EPRAP fraud was being
22 committed. To my knowledge, there have been no prior attempts to secure a search
23 warrant to search and seize these records from David.martinez.ceo@outlook.com. To my
24 knowledge, there have been no prior attempts to secure a search warrant to search and
25 seize these records from any of the other Subject Email Accounts.

26 38. Between April 17, 2023, and July 28, 2023, multiple preservation letters
27 were sent to electronic service providers to preserve the Subject Email Accounts pending
28 issuance of a court order or other legal process.

VII. CONCLUSION.

39. For the reasons set forth above, there is probable cause to believe that evidence, fruits and/or instrumentalities of Wire Fraud, in violation of Title 18, United States Code, Section 1343, will be found in the electronically stored information or communications contained and associated with the Subject Email Accounts, as well as in the subscriber and log records associated with that account. Accordingly, by this Affidavit and these Warrants, I seek authority for the government to search all of the items specified in Section I, Attachment B-1 through B-4 (attached hereto and incorporated by reference herein) to the Warrants, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment to the Warrants.



KATHLEEN MORAN
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on the 18th day of August, 2023.



BRIAN A. TSUCHIDA
United States Magistrate Judge

EXHIBIT 1

Fictitious Landlord	Fictitious Landlord's Email (Subject Email Accounts)	Fictitious Tenant	Assistance Obtained
David Martinez	1. David.martinez.ceo@outlook.com	Tenant 1 Tenant 2 Tenant 3 Tenant 4 Tenant 5 Tenant 6 Tenant 7	\$21,450.00 \$44,400.00 \$45,600.00 \$46,800.00 \$39,720.00 \$36,900.00 \$36,000.00
Shirley William (alias of Paradise Williams)	2. Shirleywilliamhomes@outlook.com 3. shirleyme63@gmail.com	Tenant 8 Tenant 9 Tenant 10 Tenant 11 Tenant 12 Tenant 13 Tenant 14 Tenant 15 Tenant 16 Tenant 17 Tenant 18 Tenant 19	\$45,300.00 \$48,360.00 \$44,820.00 \$41,700.00 \$35,750.00 \$28,920.00 \$39,120.00 \$43,000.00 \$33,960.00 \$34,308.00 \$39,900.00 Not funded
Rayvon Peterson	4. raypeterson206@outlook.com	Tenant 20 Tenant 21 Tenant 22 Tenant 23 Tenant 24	\$33,300.00 \$31,980.00 \$39,600.00 \$38,220.00 \$40,500.00
M.C.	5. malikahproperties@gmail.com	Tenant 25 Tenant 26 Tenant 27	\$39,900.00 \$42,000.00 \$36,720.00
M.H.	6. mauricehunterhomes@gmail.com	Tenant 28	\$36,360.00
Ale Cartel (alias of Jahri Cunningham)	7. cartellale@gmail.com	Tenant 29 Tenant 30 Tenant 31	\$43,740.00 \$47,400.00 \$46,200.00
A.H1.	8. AnisaHaji904@gmail.com	Tenant 32 Tenant 33	\$36,000.00 \$41,580.00
A.P.	9. Ashleymarie081590@gmail.com	Tenant 34	\$17,550.00

Fictitious Landlord	Fictitious Landlord's Email (Subject Email Accounts)	Fictitious Tenant	Assistance Obtained
Tia Robinson	10. bodiedexperience@gmail.com 11. tiarobinson437@yahoo.com	Tenant 35 Tenant 36 Tenant 37 Tenant 38 Tenant 39	\$42,000.00 \$34,308.00 \$36,000.00 \$41,160.00 Not funded
Akim Jackson (alias of D'arius Jackson)	12. akimjackson3@gmail.com	Tenant 40 Tenant 41 Tenant 42 Tenant 43 Tenant 44 Tenant 45 Tenant 46	\$40,860.00 \$41,600.00 \$39,600.00 \$47,600.00 \$43,740.00 \$43,025.00 Not funded
M.C.	13. minahcunning@gmail.com	Tenant 47 Tenant 48	\$48,360.00 \$39,900.00
S.H1.	14. Sequoyahillsestate.homes@gmail.com	Tenant 49	\$36,720.00
A.W.	15. akialwatson@gmail.com	Tenant 50	\$35,880.00
S.H2.	16. huntersandra027@gmail.com	Tenant 51 Tenant 52 Tenant 53	\$36,000.00 \$41,400.00 Not funded
A.Y.	17. amyadon2000@gmail.com	Tenant 54	\$43,050.00
I.J.	18. islynnkj@gmail.com	Tenant 55 Tenant 56 Tenant 57	\$40,800.00 \$44,160.00 \$46,080.00
K.K.	19. kowserkassa30@gmail.com	Tenant 58	\$42,900.00
A.M.	20. abdihomesguy@gmail.com	Tenant 59	Not funded
S.A.	21. samiaabdulwahab@gmail.com	Application started but not completed.	Not funded
S.M.	22. mohhsemhar916@gmail.com	Application started but not completed.	Not funded
I.W.	23. ishakayla.homes12@gmail.com	Tenant 60	\$36,900.00
T.M.	24. mtajaraye@gmail.com	Tenant 61 Tenant 62	\$36,900.00 \$36,900.00
A.H2.	25. hibbitalvina@gmail.com	Tenant 63	\$30,800.00
B.L.	26. wawoman445@gmail.com	Tenant 64	\$28,800.00
S.M.	27. shemshiameriam@yahoo.com	Tenant 65	\$44,400.00
Shaw Williams (alias of Paradise Williams)	28. shawpropertymg@yahoo.com	Tenant 66 Tenant 67 Tenant 68 Tenant 69 Tenant 70	\$30,900.00 \$30,900.00 \$34,920.00 \$30,900.00 \$28,500.00

Fictitious Landlord	Fictitious Landlord's Email (Subject Email Accounts)	Fictitious Tenant	Assistance Obtained
		Tenant 71	\$30,900.00
		Tenant 72	\$40,680.00
		Tenant 73	\$42,600.00
		Tenant 74	\$37,800.00
T.H.	29. terrellhouston123@yahoo.com	Tenant 75	\$36,660.00
R.J.	30. jacksonrodney206@yahoo.com	Tenant 76	\$26,520.00
Q.H.	31. qubahawkins1991@icloud.com	Tenant 77	\$33,708.00

ATTACHMENT A-3
Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the following Outlook accounts:

- 1. David.martinez.ceo@outlook.com**
- 2. Shirleywilliamhomes@outlook.com**
- 3. raypeterson206@outlook.com**

as well as all other subscriber and log records associated with the accounts, which are located at premises owned, maintained, controlled or operated by Microsoft Corporation, an email provider headquartered at One Microsoft Way, Redmond, Washington, 98052.

ATTACHMENT B-3

ITEMS TO BE SEIZED

I. Items to be Provided by Microsoft Corp.

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Microsoft Corp., regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Microsoft, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Microsoft is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

a. The contents of all emails associated with the accounts **from August 1, 2021, to February 28, 2022**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email. The contents of all communications and related transactional records for all Provider services used by the subscriber(s)/user(s) of the email account such as (i) email services, calendar services, file sharing or storage services, photo sharing or storage services, instant messaging or chat services, voice call services, or remote computing services, including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; (ii) attachments to communications (including native files); (iii) source and destination addresses and header or routing information for each communication (including originating Internet Protocol ("IP") addresses of e-mails; (iv) the date, size and length of each communication; and (v) any user or device identifiers linked to each communication (including cookies);

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, alternative e-mail addresses provided during registration, means and source of payments (including any credit cards or bank account numbers) and other identifiers, records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), the date on which the account was created, the length of service and the types of services utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, methods of connecting, and server log files, methods of connecting, and server log files, the IP address used to register the account, log-in IP addresses associated with session times and dates, server log files;

1 c. Basic subscriber records and login history (including, as described in 18
2 U.S.C. §2703(c)(2), names, addresses, records of session times and durations, length of
3 service and types of service utilized, instrument numbers or other subscriber numbers or
4 identities, and payment information) concerning any email account (including both
5 current and historical account) ever linked to the email account by common email
6 addresses (such as common recovery e-mail address), or a common telephone number,
7 means of payment (*e.g.* credit card number), registration or login IP addresses (during
8 one-week period), registration or login cookies or similar technologies, or any other
9 unique device or user identifier;

10 d. All records and other information concerning any document, or other
11 computer file created, stored, revised, or accessed in connection with the account or by
12 the subscriber(s)/user(s) of the account, including: (i) the contents and revision history of
13 each document or other computer file, and all records and other information about each
14 connection made to or from such document or other computer file, including the date,
15 time, length, and method of connection; (ii) server log records; (iii) data transfer volume;
16 and (iv) source and destination IP addresses and port numbers;

17 e. All records pertaining to devices associated with and used to create and
18 access the account, including device serial numbers, instrument numbers, model
19 types/numbers, International Mobile Equipment Identities (“IMEI”), Mobile Equipment
20 Identifiers (“MEID”), Global Unique Identifiers (“GUID”), Electronic Serial Numbers
21 (“ESN”), Android Device IDs, phone numbers, Media Access Control (“MAC”)
22 addresses, operating system information, browser information, mobile network
23 information, information regarding cookies and similar technologies, and any other
24 unique identifiers that would assist in identifying any such device(s);

25 f. All records or other information stored by an individual using the account,
26 including address books, contact and buddy lists, calendar data, pictures, and files, and
27 search histories;

28 g. All records pertaining to communications between the Provider and any
person regarding the account, including contacts with support services and records of
actions taken;

h. All information held by Provider related to the location and location history
of the user(s) of the account, including geographic locations associated with the account
(including those collected for non-Provider based applications), IP addresses, Global
Positioning System (“GPS”) information, and information pertaining to nearby devices,
Wi-Fi access points, and cell towers; and

i. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

Microsoft is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be Seized

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. 1343, those violations occurring between August 1, 2021, and February 28, 2022, including, for each account or identifier listed on Attachment A-3, information pertaining to the following matters:

1. Applications and supporting documents involving the King County Eviction Prevention and Rental Assistance Program (EPRAP);

2. Communications with King County, and/or King County employees, representatives, or contractors regarding EPRAP applications;

3. Communications involving the ownership of any property associated with EPRAP applications;

4. Records related to any tenants associated with EPRAP applications;

5. Communications among or between Paradise Williams, D'arius Jackson, Jahri Cunningham, Tia Robinson, Rayvon Peterson, David Martinez, and other individuals regarding EPRAP applications;

6. Communications among or between Paradise Williams, D'arius Jackson, Jahri Cunningham, Tia Robinson, Rayvon Peterson, David Martinez, and other individuals relating to the distribution of any proceeds or payments related to EPRAP disbursements;

7. All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the accounts specified, or who exercise in any way any dominion or control over the specified accounts.

8. Any address lists or buddy lists associated with the specified accounts;

1 9. All subscriber records associated with the specified accounts,
2 including name, address, local and long distance telephone connection records, or records
3 of session times and durations, length of service (including start date) and types of
4 service utilized, telephone or instrument number or other subscriber number or identity,
5 including any temporarily assigned network address, and means and source of payment
6 for such service) including any credit card or bank account number;

7 10. Any and all other log records, including IP address captures,
8 associated with the specified accounts;

9 11. Any records of communications about issues relating to the email
10 accounts, such as technical problems, billing inquiries, or complaints from other users
11 about the specified accounts. This to include records of contacts between the subscriber
12 and the provider's support services, as well as records of any actions taken by the
13 provider or subscriber as a result of the communications;

14 12. Any deleted emails, documents, information, or communications
15 that were created or deleted in furtherance of the crimes under investigation, or any other
16 communications that the Provider may retain and any records or information associated
17 with efforts to delete those emails or communications—including the dates on, and IP
18 addresses from which any efforts to delete were made;

19 13. The identity of persons who communicated with the email account
20 about matters relating to EPRAP applications, including records that help reveal their
21 whereabouts;

22 14. Information that constitutes evidence concerning persons who
23 collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the
24 criminal activity under investigation;

25 15. Information that constitutes evidence indicating the email account
26 user's state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or
27 planning, related to the criminal activity under investigation;

28 16. Technical infrastructure used in the commission of the criminal
activity under investigation;

 17. The existence of and identifiers for other email accounts, domains,
remote computing storage locations, physical storage locations, and/or physical
computers created, used or maintained by anyone participating in the activity described in
the Affidavit;

1 18. Preparatory steps taken in furtherance of the criminal activity under
2 investigation;

3 19. Attempts and conspiracies to commit the criminal activity under
4 investigation; and

5 20. All other information relating to the allegations in the Affidavit, the
6 offenses described in the Affidavit, and any issues relevant to the allegations and offense
7 described in the affidavit, including but not limited to proof of motive, opportunity,
8 intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident
9 with respect to the conduct under investigation; all other information relating to the
10 identification and location of additional evidence relating to any of the foregoing matters
11 described in this attachment; and all other information relating to the use, location,
12 ownership, transfer, and/or disposition of evidence, funds, or other assets.

13 This warrant authorizes a review of electronically stored information, communications,
14 other records and information disclosed pursuant to this warrant in order to locate
15 evidence, fruits, and instrumentalities described in this warrant. The review of this
16 electronic data may be conducted by any government personnel assisting in the
17 investigation, who may include, in addition to law enforcement officers and agents,
18 attorneys for the government, attorney support staff, and technical experts. Pursuant to
19 this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the
20 custody and control of attorneys for the government and their support staff for their
21 independent review.
22
23
24
25
26
27
28